JOURNAL OF NUMBER THEORY 2, 329–332 (1970)

Preassigned Character Values in the Gaussian Integers*

JOHN R. RABUNG

Mathematics Research Center, Naval Research Laboratory, Washington, D. C. 20390

Communicated by S. Chowla

Received October 10, 1969

Let $\gamma_1, \gamma_2, \ldots, \gamma_t$ be distinct prime Gaussian integers. With k an odd positive rational integer, take $\omega_1, \omega_2, \ldots, \omega_t$ to be k-th roots of unity, not necessarily distinct nor primitive. We show there exist infinitely many prime Gaussian integers π having a k-th-power character χ such that $\chi(\gamma_i) = \omega_i$, $1 \leqslant i \leqslant t$.

In 1963 W. H. Mills [1] gave conditions under which there exist primes having k-th power characters with certain preassigned values. It is our objective in this paper to extend Mills' result, for odd powers only, to the Gaussian integers. We shall argue in much the same manner as Mills did, but with necessarily different approaches in key places. Our main result will be

THEOREM 1. *Let k be odd. Taking $\gamma_1, \gamma_2, \ldots, \gamma_t$ to be distinct prime Gaussian integers and $\rho_1, \rho_2, \ldots, \rho_t$ to be k-th roots of unity, then there exist an infinite number of Gaussian prime numbers π for which there is a k-th-power character χ satisfying $\chi(\gamma_i) = \rho_i$, $1 \leqslant i \leqslant t$.*

This theorem, like the one for the rational case, relies entirely on the Tschebotareff density theorem (see, e.g. [2]). We shall state a special case of this theorem, but first we need some notation. We denote the quotient field of the Gaussian integers by R. Letting k be odd throughout, we take ρ to be a primitive k-th root of unity. Let $F = R(\rho)$. Taking $\alpha_1, \alpha_2, \ldots, \alpha_t$ to be nonzero elements of F, β_i will denote a root of $X^k - \alpha_i$, $1 \leqslant i \leqslant t$, and $E = F(\beta_1, \beta_2, \ldots, \beta_t)$. Clearly E is a Galois extension of F, so we let G be the Galois group of E over F. Also, we take $\rho_1, \rho_2, \ldots, \rho_t$ to be k-th roots of unity, not necessarily primitive. With this notation we have the following result by Tschebotareff:

* This paper is a portion of the author's Ph.D. Thesis done at Washington State University, Pullman, Washington.

641/2/3-6

THEOREM 2. *If there is a σ in G such that*

$$\sigma(\beta_i) = \rho_i \beta_i , \qquad 1 \leqslant i \leqslant t, \tag{1}$$

then there exist an infinite number of prime ideals $\mathfrak{p}$ of the first degree in F such that

$$\left(\frac{\alpha_i}{\mathfrak{p}}\right) = \rho_i , \qquad 1 \leqslant i \leqslant t, \tag{2}$$

where $(\alpha/\mathfrak{p})$ is the k-th power residue symbol.

We wish to use a more convenient form of condition (1). To do this we use the following lemma, also employed by Mills.

LEMMA. *Under the conditions of Theorem 2 and letting*

$$F^k = \{\alpha^k : \alpha \in F, \alpha \neq 0\},$$

the following statements are equivalent:

(a) *There exists a σ in G such that $\sigma(\beta_i) = \rho_i \beta_i$, $1 \leqslant i \leqslant t$.*

(b) *If $m_1, m_2, \ldots, m_t$ are rational integers such that*

$$\prod \alpha_i^{m_i} \in F^k, \qquad \text{then} \quad \prod \rho_i^{m_i} = 1.$$

Of course, if $\alpha_1, \alpha_2, \ldots, \alpha_t$ are in R, then statement (b) *is equivalent to*

(c) *If $m_1, m_2, \ldots, m_t$ are nonnegative rational integers such that*

$$\prod \alpha_i^{m_i} \in R \cap F^k, \qquad \text{then} \quad \prod \rho_i^{m_i} = 1.$$

The k-th-power characters modulo a Gaussian prime π are homomorphisms of the multiplicative group of Gaussian integers modulo π onto the group of k-th roots of unity. This means that the norm of π is of the form $kN + 1$. Further, these characters are the mappings given by $\chi(\gamma) = (\gamma/\mathfrak{p})$ where γ is a Gaussian integer and $\mathfrak{p}$ is a prime ideal in F which divides π. Since every prime ideal of the first degree (over R) in F is either ramified or divides a prime π whose norm is of the form $kN + 1$, we get from Theorem 2 and the above remarks:

THEOREM 3. *Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be nonzero members of R and let $\rho_1, \rho_2, \ldots, \rho_t$ be k-th roots of unity. Then if condition* (c) *holds, there exist infinitely many primes π, each having a k-th-power character χ such that $\chi(\alpha_i) = \rho_i$, $1 \leqslant i \leqslant t$.*

Up to this point we have been following Mills' development very closely. It is here that it becomes necessary to depart from his argument. Although the result to be proved is essentially the same, Mills' method of proof clearly does not extend to our case.

We intend to show that $R \cap F^k = R^k$ where $R^k = \{\gamma^k : \gamma \in R, \gamma \neq 0\}$. This will be the final step in the proof of Theorem 1. For if $\alpha_1, \alpha_2, \ldots, \alpha_t$, in Theorem 3 are taken to be Gaussian primes and if $R \cap F^k = R^k$ then condition (c) certainly holds, and we have the result. The following lemma will allow us to use proof by induction to show $R \cap F^k = R^k$.

LEMMA. *Let k be an odd positive rational integer. Let K be a field of characteristic zero containing no nontrivial k-th roots of unity, and let ρ be a primitive k-th root of unity. Suppose n divides k. Then if $\beta \in K(\rho)$ and $\beta^n \in K$, we must have $\beta \in K(\rho^{k/n})$.*

Proof. Consider the extension $K(\beta)$. Since $K(\beta) \subset K(\rho)$, this extension is Abelian. Thus, all of the conjugates of β will be in $K(\beta)$. And since

$$X^n - \beta^n = \prod_{i=0}^{n-1} (X - \beta\zeta^i) \text{ in } K(\rho)[X],$$

where ζ is taken to be a primitive n-th root of unity, we have that the conjugates of β over K will be of the form

$$\beta = \beta\zeta_0, \beta\zeta_1, \beta\zeta_2, \ldots, \beta\zeta_{m-1} \qquad \text{with} \quad m = [K(\beta) : K]$$

and ζ_i an n-th root of unity, $0 \leqslant i \leqslant m - 1$.

Thus, $K(\zeta_1, \zeta_2, \ldots, \zeta_{m-1}) \subset K(\beta)$. Also, $K(\zeta_1, \ldots, \zeta_{m-1}) = K(\omega)$ where ω is some n-th root of unity.

Suppose $K(\omega) \neq K(\beta)$. Then taking H to be the Galois group of $K(\beta)$ over K, there exists $\sigma \in H$ such that σ is not the identity, but σ holds $K(\omega)$ fixed. Let $\tau \in H$ and suppose $\tau(\beta) = \beta\zeta_j$ and $\sigma(\beta) = \beta\zeta_i$ with i, j such that $1 \leqslant i \leqslant m - 1$, $0 \leqslant j \leqslant m - 1$. Then since H is Abelian,

$$\sigma(\tau(\beta)) = \tau(\sigma(\beta))$$

or

$$\beta\zeta_i\zeta_j = \tau(\zeta_i)\, \beta\zeta_j .$$

That is, $\zeta_i = \tau(\zeta_i)$. But τ was an arbitrary member of H. Hence, $\zeta_i \in K$. This is a contradiction since K contains no nontrivial k-th roots of unity. Thus, $K(\beta) = K(\omega) \subset K(\rho^{k/n})$ since $\rho^{k/n}$ is a primitive n-th root of unity. Q.E.D.

The next lemma shows $R \cap F^k = R^k$ and will complete the proof of Theorem 1.

LEMMA. *Let K, ρ, k be as in the preceding lemma. Then if $\beta \in K(\rho)$ and $\beta^k \in K$, there exists a root of $X^k - \beta^k$ in K.*

Proof. In $K(\rho)[X]$,

$$X^k - \beta^k = \prod_{i=0}^{k-1} (X - \beta\rho^i) \tag{3}$$

And because $[K(\beta) : K] \leqslant [K(\rho) : K] \leqslant \phi(k) < k$, we have in $K[X]$

$$X^k - \beta^k = \prod_{j=1}^{l} f_j(X)$$

where $l \geqslant 2$ and the f_j's are irreducible in $K[X]$. Since the f_j's will be made up of factors in (3), each f_j will have a constant term of the form

$$\beta^{r_j}\rho^{s_j} \in K.$$

Suppose

$$(r_1, k) = n < k, \tag{4}$$

where "(,)" denotes greatest common divisor. Then there exist rational integers λ and μ such that $\lambda r_1 + \mu k = n$. And so

$$(\beta^{r_1}\rho^{s_1})^{\lambda}(\beta^k)^{\mu} = \beta^n\rho^m, \qquad \text{where} \quad m = \lambda s_1 .$$

That is, $\beta^n\rho^m \in K$. So if $n = 1$, we are done. In particular, the result is established if k is a prime number, for then $n = 1$.

To get the result for all odd k we use induction. Assume the result holds for all divisors n' of k with $n' < k$. Suppose, too, that $n > 1$ in (4) and, say, $an = k$. Then $(\beta^n\rho^m)^a = \beta^k\rho^{am} \in K$. But since K contains no nontrivial k-th roots of unity, we must have $\rho^{am} = 1$. That is, $am \equiv 0 \pmod{k}$. This gives $m \equiv 0 \pmod{n}$. Hence, $\beta^n\rho^m = (\beta\rho^c)^n$, where $cn = m$. But now by the preceding lemma $\beta\rho^c \in K(\rho^{k/n})$. The induction assumption now gives us that there exists a root of $X^n - (\beta\rho^c)^n$ in K. Such a root will also be a root of $X^k - \beta^k$. Thus, by induction, the lemma is established.

Q.E.D.

REFERENCES

1. W. MILLS, Characters with preassigned values, *Canad. J. Math.* **15** (1963), 169–171.
2. H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, "Physica-Verlag," Würzburg, Germany, 1965.